DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

DAVID COUNTRYMAN (CABN 226995)
CHRIS KALTSAS (NYBN 5460902)
CLAUDIA QUIROZ (CABN 254419)
WILLIAM FRENTZEN (LABN 24421)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7303
FAX: (415) 436-7234
david.countryman@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. Approximately 69,370 Bitcoin (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV), and Bitcoin Cash (BCH) seized from 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbh; Defendant.	CASE NO. COMPLAINT FOR FORFEITURE

NATURE OF THE ACTION

1. This is a judicial forfeiture action, as authorized by 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C), 981(b), and 21 U.S.C. § 881(a)(6), involving the seizure of the following property:

- Approximately 69,370.22491543 Bitcoin (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV), Bitcoin Cash (BCH), obtained from 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbh;

(hereinafter, collectively, the "Defendant Property"), as property constituting, or derived from, any proceeds of 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1030(a)(2) and (a)(4) (Computer Hacking), property furnished or intended to be furnished by a person in exchange for a controlled substance, or money traceable to such an exchange, or money used or intended to be used to facilitate such a violation (Narcotics Sales), and property involved in violations of 18 U.S.C. § 1956 and 1956(h) (Money Laundering and Conspiracy), and thereby forfeitable pursuant to 18 U.S.C. §§ 981(a)(l)(A), 981(a)(1)(C), 981(b), and 21 U.S.C. § 881.

JURISDICTION AND VENUE

2. This Court has jurisdiction under 28 U.S.C. §§ 1345 and 1355(a), and 18 U.S.C. §§ 981(a)(l)(A), 981(a)(1)(C), 981(b), and 21 U.S.C. § 881.

3. Venue is proper because the defendant currency was seized in the Northern District of California. 28 U.S.C. §§ 1355(b) and 1395.

4. Intra-district venue is proper in the San Francisco Division within the Northern District of California.

PARTIES

5. Plaintiff is the United States of America.

6. The Defendant Property is approximately 69,370.22491543 Bitcoin (BTC), 69,370.10730857 Bitcoin Gold (BTG), 69,370.10710518 Bitcoin SV (BSV), and 69,370.12818037 Bitcoin Cash (BCH), obtained from 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbh on or about November 3, 2020.

FACTS

7. From 2011 until October 2013, when it was seized by law enforcement, Silk Road was the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were bought and sold regularly by the site's users. While in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars derived from these unlawful transactions.

8. For example, contemporaneous with its seizure, there were nearly 13,000 listings for controlled substances on the website, listed under the categories "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants," among others. Clicking on the link for a particular listing brings up a picture and description of the drugs being offered for sale, such as "HIGH QUALITY #4 HEROIN ALL ROCK" or "5gr UNCUT Crystal Cocaine!!".

9. During its operation, law enforcement agents made over 100 individual undercover purchases of controlled substances from Silk Road vendors. The substances purchased in these undercover transactions have been various Schedule I and II drugs, including ecstasy, cocaine, heroin, LSD, and others. Samples of these purchases were laboratory-tested and have typically shown high purity levels of the items that were advertised by Silk Road. Based on the postal markings of the packages in which the drugs arrived, these purchases appear to have been filled by vendors located in over ten different countries, including the United States. Law enforcement agents also made undercover purchases of hacking services on Silk Road, including purchases of malicious software such as password stealers and remote access tools.

10. Contemporaneous with the seizure of Silk Road, there were 159 listings on the site under the category "Services." Most concerned computer services: for example, one listing was by a vendor to hack into Facebook, Twitter, and other social networking accounts of the customer's choosing, offering that "You can Read, Write, Upload, Delete, View All Personal Info"; another offered tutorials teaching "22 different methods" for hacking ATM machines. Other listings offered services that were likewise criminal in nature. For example, one listing was for "HUGE Blackmarket Contact List," which described lists of "connects" for "Services" such as "Anonymous Bank Accounts," "Counterfeit Bills (CAD/GBP/EUR/USD)," "Firearms + Ammunition," "Stolen Info (CC [credit card], Paypal)," and "Hitmen (10+ countries)."

11. The only form of payment accepted on Silk Road was Bitcoin.

12. All told, Silk Road generated sales revenue totaling over 9.5 million Bitcoin, and collected commissions from these sales totaling over 600,000 Bitcoin.

13. Silk Road used a so-called "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Blockchain. According to the Silk Road

wiki web page, Silk Road's tumbler "sends all payments through a complex, semi-random series of dummy transactions, . . . making it nearly impossible to link your payment with any coins leaving the site." In other words, if a buyer makes a payment on Silk Road, the tumbler obscures any link between the buyer's Bitcoin address and the vendor's Bitcoin address where the Bitcoins end up—making it fruitless to use the Blockchain to follow the money trail involved in the transaction, even if the buyer's and vendor's Bitcoin addresses are both known. The only function served by Silk Road's implementation of such "tumblers" is to assist with the laundering of criminal proceeds.

14. In February 2015, a federal jury convicted Silk Road creator Ross Ulbricht on seven counts including conspiracy to distribute narcotics and money laundering. Ulbricht had moved to San Francisco, within the Northern District of California, prior to his arrest and was operating Silk Road from the Northern District of California. He was arrested in San Francisco and processed through the United States District Court for the Northern District of California before being removed to the Southern District of New York for prosecution.

15. In 2020, law enforcement officers used a third party bitcoin attribution company to analyze Bitcoin transactions executed by Silk Road. From this review they observed 54 transactions that were sent from Bitcoin addresses controlled by Silk Road, to two Bitcoin addresses: 1BADznNF3W1gi47R65MQs754KB7zTaGuYZ and 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN totaling 70,411.46 BTC (valued at approximately $354,000 at the time of transfer).

16. The individual amounts that were transferred were mainly round Bitcoin amounts and close together in time. For example, 10 of the transfers occurred at approximately 3:59 a.m. and each transfer was for exactly 2,500 Bitcoin. This pattern of withdrawals and the amount that was withdrawn was not typical for a Silk Road user. Specifically, a review of other withdrawals from Silk Road revealed Bitcoin amounts that were mostly less than 100 Bitcoin. These 54 transactions were not noted in the Silk Road database as a vendor withdrawal or a Silk Road employee withdrawal and therefore appear to represent Bitcoin that was stolen from Silk Road.

17. On approximately April 9, 2013, the Bitcoin addresses that received the 70,411.46 Bitcoin from Silk Road sent 69,471.082201 (approximately $14 million at the time of transfer) to 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx (hereafter "1HQ3").

18. On approximately April 23, 2015, 1HQ3 sent 101 Bitcoin (approximately $23,700) to BTC-e, a company that provided Bitcoin related services and operated as an unlicensed cryptocurrency exchange. In January 2017, BTC-e and a Russian operator of BTC-e were indicted in the Northern District of California for operating an unlicensed money transmitting business and for money laundering through the exchange.

19. Between April 2015 and November 2020, the remainder of the funds, 69,370.082201 BTC, remained in 1HQ3.[1] As of November 3, 2020, 1HQ3 had a balance of 69,370.22491543 Bitcoin (valued at approximately $1 Billion as of November 4, 2020).

20. In August 2017, Bitcoin split into two cryptocurrencies, commonly known as a hard fork. Hard fork coin splits are created via changes of the blockchain rules and share a transaction history with Bitcoin up to the time of the split. The first hard fork split occurred on August 1, 2017, resulting in the creation of Bitcoin Cash (BCH). When this split occurred, any Bitcoin address that had a Bitcoin balance now had the same balance on the Bitcoin blockchain and on the Bitcoin Cash blockchain. A search for 1HQ3 on the Bitcoin Cash blockchain revealed a balance of approximately 69,370.12818037 BCH prior to the Government's seizure. Much like the aforementioned hard fork of Bitcoin and BCH, there were subsequent hard forks of Bitcoin that resulted in the creation of Bitcoin Gold (BTG) and Bitcoin SV (BSV). Review of the BTG and BSV blockchains revealed that 1HQ3 held a balance of 69,370.10730857 BTG and 69,370.10710518 BSV prior to the Government's seizure.

21. Individual X, whose identity is known to the government, was determined to have been involved in a transaction that related to 1HQ3.

22. According to an investigation conducted by the Criminal Investigation Division of the Internal Revenue Service and the U.S. Attorney's Office for the Northern District of California, Individual X was the individual who moved the cryptocurrency from Silk Road. According to the investigation, Individual X was able to hack into Silk Road and gain unauthorized and illegal access to Silk Road and thereby steal the illicit cryptocurrency from Silk Road and move it into wallets that

[1] Because Bitcoin addresses are public, individuals are able to identify Bitcoin addresses with large balances. Individuals will often send minimal amounts of Bitcoin to these addresses for unknown reasons. For example, on November 3, 2020, 1HQ3 received 0.00010999 bitcoin (approximately $1.51) from an unknown individual.

Individual X controlled. According to the investigation, Ulbricht became aware of Individual X's online identity and threatened Individual X for return of the cryptocurrency to Ulbricht. Individual X did not return the cryptocurrency but kept it and did not spend it.

23. On November 3, 2020, Individual X signed a Consent and Agreement to Forfeiture with the U.S. Attorney's Office, Northern District of California. In that agreement, Individual X, consented to the forfeiture of the Defendant Property to the United States government.

24. On November 3, 2020, the United States took custody of the Defendant Property from 1HQ3.

VIOLATION

The United States incorporates by reference the allegations in paragraphs one through 24 as though fully set forth.

Title 18, United States Code, Section 981(a)(1)(A) provides for civil and criminal forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of Title 18, United States Code, Sections 1956, 1957, or 1960, and any property traceable to such property.

Title 18, United States Code, Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting a "specified unlawful activity" or a conspiracy to commit such offense. Title 18, United States Code, Sections 1956(c)(7) and 1961(1) define specified unlawful activity to include Computer Hacking, in violation of Title 18, United States Code, Section 1030, and conspiracy to commit Computer Hacking.

Title 21, United States Code, Section 881(a)(6) provides for the forfeiture of all moneys, negotiable instruments, securities, or other things of value furnished or intended to be furnished by any person in exchange for a controlled substance or listed chemical, all proceeds traceable to such an exchange and all money used or intended to be used to facilitate any violation of Subchapter I, Chapter 13, Subchapter I of Title 21 United States Code.

In light of the foregoing, and considering the totality of the circumstances, there is probable cause to believe that the Defendant Property represents proceeds traceable to computer hacking in violation 18 U.S.C. § 1030(a) and conspiracy in violation of 18 U.S.C. § 371. As such, the Defendant Property is forfeitable pursuant to 18 U.S.C. § 981(a)(l)(C). Additionally, there is probable cause to believe that the

Defendant Property represents property traceable to narcotics trafficking. As such, the Defendant Property is forfeitable pursuant to 21 U.S.C. § 881(a)(6). To the extent the Defendant Property includes funds that did not originate as proceeds from the illegal activities discussed herein, those funds were "involved in" money laundering in violation of 18 U.S.C. § 1956 because they were comingled with and used to conceal and disguise the nature, location, source, ownership or control of the criminal proceeds, or were involved in a conspiracy to launder such proceeds. Accordingly, the Defendant Property is forfeitable pursuant to 18 U.S.C. §§ 981(a)(l)(A) and 981(b).

WHEREFORE, plaintiff United States of America requests that due process issue to enforce the forfeiture of the Defendant Property; that notice be given to all interested parties to appear and show cause why forfeiture should not be decreed; that judgment of forfeiture be entered; that the Court enter judgment forfeiting the Defendant Property; and that the United States be awarded such other relief as may be proper and just.

DATED: 11/5/2020

Respectfully submitted,
DAVID L. ANDERSON
United States Attorney

__/s/ David Countryman_____
DAVID COUNTRYMAN
CHRIS KALTSAS
CLAUDIA QUIROZ
WILLIAM FRENTZEN
Assistant United States Attorneys

VERIFICATION

I, Jeremiah Haynie, state as follows:

1. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service ("IRS-CI"). I am a case agent assigned to this case. As such, I am familiar with the facts, and the investigation leading to the filing of this Complaint for Forfeiture.

2. I have read the Complaint and believe the allegations contained in it to be true.

* * * * *

I declare under penalty of perjury that the foregoing is true and correct. Executed this 4th day of November, 2020 in East Lansing, Michigan.

JEREMIAH HAYNIE
Special Agent
Internal Revenue Service - Criminal Investigation